Mittuniversitetet
MID SWEDEN UNIVERSITY

Den fullständiga studiehandledningen för DT144G Webbapplikationssäkerhet

Daniel Bosk*

studyguide.tex 1247 2013-09-03 08:06:18Z danbos

Innehåll

1 Mål

Kursens syfte är att vara förberedande för att utveckla säkra webbapplikationer, att ge en medvetenhet för behovet av säkerhet hos dessa. Kursen tar upp de mest förekommande attackerna mot webbapplikationer och metoder för att förebygga dessa.

Mer specifikt ska du efter genomgången kurs uppfylla följande mål:

- Att redogöra för de vanligaste attackerna mot webbapplikationer.

- Att förklara hur de vanligaste attackerna mot webbapplikationer fungerar.
- Att tillämpa metoder för att förebygga de vanligaste attackerna mot webbapplikationer.
- Att granska programkod för att finna säkerhetsbrister.

2 Kursupplägg

Innehållet i kursen är uppbyggt kring material från The Open Web Application Security Project (OWASP). Detta projekt arbetar generellt med säkerhet, men har sitt ursprung i webbapplikationssäkerhet. Var tredje år publicerar de en topp tio-lista [OWASP13] som är en rankad lista över de tio mest förekommande säkerhetsbristerna på webben.

Kursen består av föreläsningar, som behandlar delar av allt material som finns tillgängligt [OWASP13; Wei+05; MKC08], och handledning i ett projekt, vilket är det examinerande momentet på kursen. Föreläsningarna är uppbyggda kring bristerna som presenteras i topp tio-listan. Deltagare förutsätts därför ha en god förståelse för diverse webbteknologier för att kunna förstå föreläsningarnas innehåll. Parallellt med föreläsningarna förväntas du läsa [Wei+05] och senare även översiktligt gå igenom [MKC08] för att kunna ha som referens vid granskningen av projektet.

Kursen examineras med genomförande av ett större projekt. Det rekommenderas att du sätter igång med detta redan från början. Projektet syftar till att du ska skriva en säker webbapplikation, se lydelsen för detaljer, och du kommer att lära dig om säkerheten allteftersom kursen går.

2.1 Schema

Du finner en sammanställning av kursens schema i tabell 1 på nästa sida. Det är naturligtvis valfritt att följa detta schema sånär som på slutdatum för kursens uppgifter och när föreläsningarna ges. Läsanvisningar för respektive moment följer i kommande avsnitt. Undervisningen förutsätter att du följer dessa riktlinjer.

2.2 Introduktionsföreläsning

Föreläsningen ger en introduktion till kursen och informationssäkerhetsområdet. Den täcker ytligt kapitel 1 *What is security engineering?* i [And08], läs detta kapitel.

2.3 Projektet

Inför utvecklingen av projektet bör du ha läst till och med kapitlet ”Secure Coding Principles” i *A Guide to Building Secure Web Applications and Web Services* [Wei+05]. Därefter har du övriga kapitel som referens under utvecklingens gång.

Du ska även ha läst kapitel 1–3 i *OWASP Testing Guide* [MKC08] inför projektet. Därefter har du kapitel 4 som stöd för granskningen av ett projekt.

Kursvecka	**Arbete**
1	Kursstart/introduktion Föreläsning om injektionsattacker Projekthandledning
2	Föreläsning om felande autentisering och sessionshantering Föreläsning om cross-site scripting (XSS) Projekthandledning
3	Föreläsning om osyddade objektreferenser Föreläsning om felkonfigurerade säkerhetsmekanismer Projekthandledning Slutdatum för introduktionsuppgift
4	Föreläsning om otillräckligt skydd för känsliga data Föreläsning om utebliven åtkomstkontroll på funktionsnivå Projekthandledning
5	Föreläsning om cross-site request forgery (CSRF) Föreläsning om användning av komponenter med kända sårbarheter Projekthandledning
6	Föreläsning om ovaliderade omdirigeringar Projekthandledning
7	Projekthandledning
8	Projekthandledning
9	Projekthandledning
10	Redovisning av projekt

Tabell 1: En sammanställning av kursens moment och när de kommer att genomföras. Tiden är anpassad efter studietakt om halvfart.

2.4 Föreläsning om injektionsattacker

Föreläsningen utgår från avsnittet *A1 Injections* i [OWASP13].

2.5 Föreläsning om felande autentisering och sessionshantering

Föreläsningen utgår från avsnittet *A2 Broken Authentication and Session Management* i [OWASP13]. Innehållet i föreläsningen tar även upp delar från kapitlen "Authentication" och "Session Management" i [Wei+05], kapitel 3 "Protocols" i [And08] samt avsnitten "V1: Authentication Verification Requirements" och "V2: Session Management Verification Requirements" i [Kaz+13]. För att behandla lösenordspolicyer bör även artikeln "Of passwords and people" [Kom+11] läsas.

2.6 Föreläsning om cross-site scripting (XSS)

Föreläsningen utgår från avsnittet *A3 Cross-Site Scripting (XSS)* i [OWASP13].

2.7 Föreläsning om oskyddade objektreferenser

Föreläsningen utgår från avsnittet *A4 Insecure Direct Object References* i [OWASP13].

2.8 Föreläsning om felkonfigurerade säkerhetsmekanismer

Föreläsningen utgår från avsnittet *A5 Security Misconfiguration* i [OWASP13]. Vidare läsning är avsnitten "Error Handling, Auditing and Logging" och "Configuration" i *A Guide to Building Secure Web Applications and Web Services.*

2.9 Föreläsning om otillräckligt skydd för känsliga data

Föreläsningen utgår från avsnittet *A6 Sensitive Data Exposure* i [OWASP13]. Den behandlar även kapitel 5 "Cryptography" i *Security engineering : a guide to building dependable distributed systems* [And08] samt avsnittet "Cryptography" i *A Guide to Building Secure Web Applications and Web Services* [Wei+05]. Utöver detta bör du läsa avsnitten "V5 Cryptography at Rest Verification Requirements", "V7 Data Protection Verification Requirements", "V8 Communications Security Verification Requirements" och "V9 HTTP Security Verification Requirements" i *OWASP Application Security Verification Standard 2013* [Kaz+13].

2.10 Föreläsning om utebliven åtkomstkontroll på funktionsnivå

Föreläsningen utgår från avsnittet *A7 Missing Function Level Access Control* i [OWASP13]. Innehållet täcker också delar av kapitel 4 "Access Control" i [And08] och kapitlet "Authorization" i [Wei+05]. Du bör också läsa avsnittet "V3 Access Control Verification Requirements" i [Kaz+13].

2.11 Föreläsning om cross-site request forgery (CSRF)

Föreläsningen utgår från avsnittet *A8 Cross-Site Request Forgery (CSRF)* i [OWASP13].

2.12 Föreläsning om användning av komponenter med kända sårbarheter

Föreläsningen utgår från avsnittet *A9 Using Components with Known Vulnerabilities* i [OWASP13].

2.13 Föreläsning om ovaliderade omdirigeringar

Föreläsningen utgår från avsnittet *A10 Unvalidated Redirects and Forwards* i [OWASP13].

3 Examination

Kursen examineras med med ett projekt, se lydelsen för detaljer. Detta examineras genom en skriftlig rapport och en muntlig presentation. Projektrapporten betygsätts A–E för godkänt eller F–Fx för underkänt.

I projektet ingår även att kritiskt granska ett annat projekt ur ett säkerhetsperspektiv. Denna granskning ska resultera i skriftlig återkoppling till den som genomfört projektet, för att denne ska kunna åtgärda eventuella brister. Denna granskning ska också ligga till grund för en opponering vid projektpresentationerna. Denna del betygsätts P för godkänt eller F för underkänt.

4 Vad händer om jag ej blir klar i tid?

Slutdatumena på denna kurs är av yttersta vikt. Du måste ha genomfört introduktionsuppgiften inom dess givna slutdatum, om du inte gör detta kommer du att avregistreras från kursen och din plats kommer att ställas till förfogande för andra sökande.

Vad gäller den övriga examinationen på kursen kommer det att ges ett redovisningstillfälle under kursens gång, detta kommer att vara under ordinarie tentamensvecka. Därefter ges ytterligare två redovisningstillfällen, dessa förläggs inom ett år. Alla dessa tillfällen kommer att finnas i kursens schema (i studentportalen).

De slutdatum som finns för dessa tillfällen är strikta. Om du missar slutdatumet för ett tillfälle hänvisas du till nästa redovisningstillfälle. Efter det tredje redovisningstillfället hänvisas till redovisningstillfällena under nästkommande kursomgång.

Ingen handledning är planerad efter kursens slut, det vill säga efter det sista schemalagda handledningstillfället. Om du inte hinner bli klar med projektet inom kursens tidsramar och du vill vara garanterad handledning av lärare krävs att du omregistrerar dig på nästa kursomgång. Omregistrering på kurs sker i mån om plats, alla förstagångssökande och reserver kommer att prioriteras. Om du känner att du inte kommer att hinna bli klar med projektet är det

därför bättre att göra ett tidigt avbrott på kursen och söka om den inför nästa kurstillfälle. Tidigt avbrott kan registreras senast tre veckor från kursstart.

Referenser

[And08] Ross J. Anderson. *Security engineering : a guide to building dependable distributed systems*. 2. utg. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: http://www.cl.cam.ac.uk/~rja14/book.html.

[Kaz+13] Sahba Kazerooni, Daniel Cuthbert, Andrew van der Stock och Krishna Raja, utg. *OWASP Application Security Verification Standard 2013*. 2013. URL: http://sourceforge.net/projects/owasp/files/ASVS/OWASP%20ASVS%202013%20Beta%20_v1.0.pdf/download.

[Kom+11] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Christin Nicolas, Lorrie Faith Cranor och Serge Egelman. "Of passwords and people: Measuring the effect of password-composition policies". I: *CHI*. 2011. URL: http://cups.cs.cmu.edu/rshay/pubs/passwords_and_people2011.pdf.

[MKC08] Matteo Meucci, Eoin Keary och Daniel Cuthbert, utg. *OWASP Testing Guide*. 2008. URL: http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf.

[OWASP13] The Open Web Application Security Project. *OWASP Top 10 - 2013: The Ten Most Critical Web Application Security Risks*. Juni 2013. URL: http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf.

[Wei+05] Adrian Weismann, Mark Curphey, Andrew van der Stock och Ray Stirbei, utg. *A Guide to Building Secure Web Applications and Web Services*. 2005. URL: http://prdownloads.sourceforge.net/owasp/OWASPGuide2.0.1.pdf?download.